Fordham International Law Journal

Volume 19, *Issue* 5 1995 *Article* 7

Is International Law Ready for the Information Age?

M. E. Bowman*

*

Is International Law Ready for the Information Age?

M. E. Bowman

Abstract

This Essay discusses the challenges to protect the public from a myriad of harms related to new, and poorly understood, vulnerabilities arising from the frontier of cyberspace and how international law can offer protection against the global potential for harm.

IS INTERNATIONAL LAW READY FOR THE INFORMATION AGE?

*M.E. Bowman**

It was a seminal event that ended the carnage in 1648. The military peace that followed the Thirty Years War was a mere respite, but the Peace of Westphalia cast a measure of political stability. Westphalia was midwife to the legal concept of the nation state, sovereign within its borders. At Westphalia, an agreement[1] was crafted that memorialized and solidified the concept that physical security gives rise to international stability.

Stemming from that agreement, national borders and sovereign integrity have now been the benchmarks of stability for more than three centuries. Even today, nations reach the brink of conflict over disputed title to barren island rocks, wastelands of sand, tundra, or ice and border claims centuries old. Nations are quick to use available international fora to bristle at slights, real or imagined.

So important is the concept of sovereignty that just in our lifetimes, a multitude of conflicts have erupted in the name of Westphalian dominion. Yet, in the brief measure of our children's lives, the territorial concept of stability is being challenged. Today, economic transactions, political intercourse, and technological developments, much of which span previously im-

---

* Associate General Counsel, Federal Bureau of Investigation. The views expressed herein do not necessarily represent the views of the FBI or the Department of Justice.

1. The Congress of Westphalia (1643-48) was Europe's first great peace conference and the first international gathering of importance since the Council of Constance (1414-18). Almost every act of the treaty that ended the war emphasized the importance of the sovereign state. In practical terms, it represented the death knell of the Holy Roman Empire, gave sovereignty to German and Swiss principalities, fixed borders in France, Sweden, and the Netherlands and ushered in an era of national wars for territorial and economic aggrandizement. Beyond any doubt, it laid the formal foundations for the modern state system. For additional information on the Congress of Westphalia and the Council of Constance, see H. NEUFELD, THE INTERNATIONAL PROTECTION OF PRIVATE CREDITORS FROM THE TREATIES OF WESTPHALIA TO THE CONGRESS OF VIENNA (1648-1815) (1971); Henry Wheaton, *History of the Progress of the Law of Nations in Europe From the Peace of Westphalia to the Congress of Vienna With an Historical Notice of That Law Before the Peace of Westphalia*, 77 EDINBURGH REV. 303 (1843); PHILLIP H. STUMP, THE REFORMS OF THE COUNCIL OF CONSTANCE 1414-18 (1994).

pregnable international barriers, have become significant, even critical, to national security and international stability alike.

To take their place in world affairs today, nations require access to information, global financial markets, instantaneous communications, and other trappings of the information age. The preservation of secure borders, physical resources, and national honor remain crucial concepts of national security, but international standards and centuries of experience help us meet the daily problems of Westphalian sovereignty. In contrast, there are few international standards to deal with the burgeoning capabilities of nations and their constituents to obtain and manipulate information.

To collate, analyze, manage, and protect the data on which society has come to rely is an enormous but manageable task. Similarly, providing public access to information and communications is a daunting challenge, but one capable of resolution. The most formidable challenge is to protect the public from a myriad of harms related to new, and poorly understood, vulnerabilities arising from the frontier of cyberspace.

The vulnerabilities created by access to information, and to information architecture, outstrip by far, those of any analogous reference point in the history of civilization. Every hacker, criminal and government with the equipment, minimal expertise, and raw determination to intrude has the capability of bringing harm to both individuals and structures.

This is the electronic equivalent of terrorism or guerrilla warfare. The effect of an attack on modern information systems is not unlike the Mongol way of fighting seven centuries ago. With vastly inferior numbers, the Mongols conquered enormous territories by learning enemy strengths and vulnerabilities while keeping their own secret. Avoiding direct confrontation, they attacked the flanks and the rear of the enemy or bypassed the enemy altogether. They disrupted communications, attacked at times and places of their own choosing, and terrorized adversaries into submission. Today, cyberspace is ripe for similar tactics.

The prototype target of attack is not new. The origin of global networks, and today's Internet, is international banking and international corporate ventures. World markets created the need for globalization and that need has spawned an enormous network of communications systems. In particular, the In-

ternet geometrically expands the concept of access. It democratizes information exchange in a way that inextricably links the global community while enhancing both personal and institutional vulnerabilities.

I. *NATIONAL INFORMATION INFRASTRUCTURE*

Computers have solved the analyst's nightmare of collation of a geometrically increasing body of data. On the other hand, they have created a crucible of social, economic, and physical dependence on electronic communications. That crucible, in domestic terms, will be known as the National Information Infrastructure ("NII"). A logical step-child of the Internet, the NII is growing from existing networks to become more powerful, more necessary, and more widely used than anything we possibly could have imagined a scant few years ago.

Although still inchoate, the NII is a system composed of high-speed telecommunications networks, databases, and advanced computer systems; together these make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector, but its functional advantages are societal. In a very real sense, the NII is U.S.-style democratization. Whether domestic or global, it will ameliorate the constraints of geography, economics, and disability, giving the ordinary citizen a means of global access and personal participation that rivals the town meeting.

Already the NII is integral to many Federal programs and many Federal agencies are becoming dependent on it for execution of their missions. There is little question that the NII of the future increasingly will support a wide variety of vital programs as disparate as air traffic control and compilation of census data. Response to natural disaster and delivery of government benefits will depend on the NII. Power grids, transportation systems, financial institutions, and economic transactions all will rely on NII capabilities.

Information truly is the critical infrastructure of modern society. U.S. information capabilities have exposed North Korean nuclear weapons programs, uncovered Russian and Chinese nuclear dealings with Iran, and facilitated U.N. weapons inspections in Iraq. These same capabilities turn as easily to non-mili-

tary benefits such as discerning environmental dangers, advancing agricultural research, or facilitating medical studies.

Thanks to Cold War investments in information processing capabilities, the United States has an unparalleled capability to integrate complex information systems, but this is a transitory monopoly. Information dependence is a growing global phenomenon that directly affects military, political, economic, and social resources alike. In some cases, the strengths of these traditional resources are diminished, in others they are enhanced; each transition represents an evolution of global interdependence. At minimum, this means it is in the U.S. interest to promote a common information infrastructure with standard reference points. Only in commonality can security and international cooperation be assured.

Unfortunately, vulnerabilities are inherent within these benefits. Public safety and the national defense call for a somewhat anomalous need, a secure NII. Access, not security is both the purpose and the hallmark of the NII. Individual privacy, public speech, private enterprise, all cherished aspects of American life, are social, if not legal, barriers to regulation and investigation alike. Even in formative stages, the NII is sparking a debate over dichotomous public interests.

II. *NII VULNERABILITY*

Profit and peril are the reciprocals of NII access; the benefits we obtain all yield a vulnerability. We enjoy the facility of electronic banking, but security experts estimate that sophisticated "hackers" commit some thirty-six electronic bank robberies of US$1 million or more each year.[2] Even the sophisticated technology of our intelligence agencies may be inadequate. As one former official stated, "[f]oreign intelligence services have gained access to classified information in U.S. computers by remote means . . . and we have done the same thing to them."[3]

As a nation we possess the most formidable fighting capability in the world, but one dependent on computer security. Artillery and rockets are directed by computers, our armies are guided to precise locations by satellite communications, and mil-

2. *That Wild, Wild Cyberspace Frontier*, INFO. WAR & CYBERSPACE SEC., Fall 1995, at 1.

3. Jay Peterzell, *Spying and Sabotage by Computer*, TIME, Mar. 20, 1989, at 25; *see Soviet Computer Woes Raise Espionage Threat*, ADVANCED MIL. COMPUTING, Sept. 29, 1988, at 1.

itary aircraft have software programs exceeding half a million lines of logic. This dependence creates a unique opportunity for undetected algorithmic sabotage, computer spoofing, or both. Dependence on computer logic means that the failure to anticipate a problem will yield a technological vulnerability. During the Falklands-Malvinas conflict, when two Argentine aircraft on closely parallel courses attacked a British warship, the British Sea Wolf missile defense system was unable to cope with an unanticipated attack profile.[4] Unable to handle the situation, the software shut down automated systems, leaving the ship virtually defenseless.

Public safety depends in many ways on electronic communications. The Federal Aviation Administration ("FAA") diligently maintains a mantle of safety in increasingly crowded skies, but it depends on computers. An unfriendly power or terrorist group could develop the capability for a devastating, concerted attack on FAA computers nationwide. Recently, the radars at the busy Pittsburgh airport were blinded for six full minutes,[5] giving us a snapshot of what a test of a capability to attack that system could be like.

We enjoy the ability to summon rapidly emergency police or rescue aid by dialing 911, but that too is a severable lifeline. This became apparent in 1991-92 when a computer attack utilizing multistate switching overloaded the Virginia and Maryland 911 systems with spurious calls. Since then, intruders have learned that they can frustrate investigation by attacking through multinational switching.

Further, it does not require the resources of a government to penetrate even "secure" computer systems. To take advantage of computer technology, communications systems have been melded together by a patchwork system of hardware and software technology and the common telephone. Computer-to-computer communications yield enormous benefit, but also a quantitative increase in the vulnerability of individual systems. This has been highlighted in recent years by computer hackers who have gained notoriety for their intrusions into the computer

4. Boorman & Levitt, *Software Warfare and Algorithm Sabotage*, SIGNAL, May 1988, at 75.

5. *Pittsburgh Airport's Radar Screens Go Out for 6 Minutes*, CHARLESTON GAZETTE, Feb. 1, 1996, at 6A.

systems of others, particularly government-associated computer systems. These are serious vulnerabilities. The individual event itself, even if successful, may be wholly clandestine, making it difficult or impossible even to know the penetration has occurred. Unlike theft of tangible property, information stored electronically may be retrieved and copied an infinite number of times without leaving evidence of the intrusion.

Hackers, whose intentions may range from benign to destructive, are the progenitor problem. "Hacking" gained notoriety when the Chaos Computer Club broke into NASA computers in 1987,[6] generating fear as much for the ability to put "viruses" into the computer systems as for the potential to withdraw sensitive information. The complexity of the problem became apparent after it required the dogged, months-long effort of an astronomer and computer expert to prove to government officials that some forty government systems had been penetrated from abroad. In the end, the astronomer's efforts proved that a group of West German hackers, possibly in the employ of East bloc intelligence agents, were responsible.

When even the ability to control level flight is computer dependent, there is the possibility that effective warfighting may be waged, or preparedness inhibited, merely by tampering with computer or associated software systems.[7] Similarly, the effect of undetected defects could be disastrous for warfighting, transportation systems, flood control, or economic institutions.

Even the harmless virus inserted by "friendly" hackers can be both fiscally and physically destructive. In a case that captured the headlines, a relatively benign virus, intended only to spread a "worm" across the Internet, replicated faster than expected, quickly shutting down the entire system.[8] The potential

---

6. Keith Stone, *Cyberspace Crawls with Crooks, Spies, Computer Cops Warn*, HOUS. CHRON., Sept. 11, 1994, at C9.

7. *See* Peter Grant & Robert Richie, *The Eagle's Own Plume, in* NAVAL INST. PROC., July 1983. Aircraft have, in fact, crashed due to software design defects. One author suggests that the crash of two U.S. Air Force F-117 stealth fighters in identical, suspicious circumstances, might suggest a "bug" in the software. A worse problem will be logic bombs, or viruses bugs. *See* Stefan Geisenheyner, *The Dangers Lurking in Military Software Production: Viruses, Trojan Horses and Logic Bombs*, ARMADA INT'L, Oct.-Nov. 1989, at 22.

8. SCIENCE APPLICATIONS INT'L CORP., INFORMATION WARFARE: LEGAL, REGULATORY, POLICY AND ORGANIZATIONAL CONSIDERATIONS FOR ASSURANCE 2-7 (1995); Loring Wirbel, *Swat Team for Viruses*, ELECTRONIC ENG. TIMES, Dec. 12, 1988, at 17.

for the virus, logic bomb, or algorithmic sabotage to create chaos in computer systems is so great that in 1988 the Pentagon temporarily severed the connections between Department of Defense computers and a corporate computer network that had been compromised..

The potential for intrusion has not appreciably diminished. The Defense Information Security Agency ("DISA") recently reported that 88% of defense computer systems are easily penetrated.[9] Of the successful penetrations it conducted, 96% were not detected.[10] Equally disturbing, of those detected, 95% were not reported,[11] perhaps because hacking incidents have not yet been compelling. DISA continues to report possible intrusions of government computer systems numbering in the thousands.

III. *PROTECTING THE NII*

As distressing as these statistics may be, they can mislead the reader. This vulnerability is not one solely affecting government or big business. Individuals also may be harmed directly by NII attacks. By attacking individual data files, it is possible to steal or corrupt personal records such as health, education, consumer purchases, tax filings, or credit history. Put simply, this is electronic terrorism.

Beyond cavil, there exists a need for effective law and oversight of both the NII itself and of public safety-related uses of the NII. A sound legal system that applies both civil and criminal penalties is essential. Existing laws provide some protection, but the harms to be prevented challenge both application and enforcement as technology increasingly facilitates familiar crimes and generates new ones.[12] The NII will be used to smuggle stolen corporate information, to transmit child pornography, to sabotage industrial or financial databases, to electronically stalk,

---

9. *See* Neil Munro, *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, WASH. POST, July 16, 1995, at C3 (reporting statements of Robert Ayers, Chief of DISA's Warfare Division).

10. *Id.*

11. *Id.*

12. The U.S. Government recognized at the turn of the century that the telecommunications infrastructure was critical to national security and economic progress. Since then, there have been many communications-related laws and regulations enacted. Even so, technology has far outstripped the legal and regulatory scheme of the United States. For most of the World, legal protection in this area is sadly deficient.

threaten, or to perpetrate fraud. All of these capabilities, as nations are rapidly discovering, transcend national boundaries.

Media issues today are diverse, sometimes arcane, sometimes bizarre, and ever increasing in complexity. Not long ago, a Pakistani cleric asked the U.S. Department of State to extradite Madonna and Michael Jackson because their music violates Islamic law. We might be amused by that sort of request, but the underlying social and cultural issues are serious.

In the United States, an attempt to protect children with a legislative ban on "indecent" material was, as expected, blocked by a federal judge to ensure protection of constitutional values. France recently banned a book that violated its laws, only to find that same book immediately available on the Internet. Germany unsuccessfully has resisted both pornography and racial hatred messages on the Internet. China, ethnocentrically, is trying to insulate its citizenry by excluding the Internet and creating an indigenous version.

These are but a taste of the future. The explosion of cyberspace activities gives rise to vulnerabilities that reach into the entire social spectrum. The potential villains are hackers,[13] disgruntled employees, criminals,[14] terrorists, commercial organizations,[15] and even nations.[16] To complicate matters further, cyberspace attacks are virtually indistinguishable one from another. Even if adequate laws and technological safeguards did exist, the anonymous nature of an intrusion would make it difficult to prioritize investigations.

It will be difficult, perhaps even impossible, to know whether an intrusion represents the exuberance of a curious, youthful hacker or a test of destructive information warfare capabilities. At best, the distinctions between "crime" and "warfare," "accident" and "attack" will be blurred. The resources for mayhem in cyberspace are within reach of virtually every aspect of

---

13. One hacker lifted 20,000 credit card numbers from various systems before he was tracked down by a computer security expert who had been provoked by the hacker.

14. An electronic Clyde Barrow, working from St. Petersburg, invaded a Citibank computer and stole more than US$10 million. *Russians Arrest 6 in Computer Thefts*, N.Y. TIMES, Sept. 27, 1995, at D5.

15. Almost daily, commercial organizations report instances of economic espionage and theft.

16. Recently, the Russian Government acknowledged that its espionage apparatus was being turned increasingly to the acquisition of foreign technology.

domestic and international society, and few users understand, and many choose not to accept, any need for communal responsibility.

Certainly, the United States needs to consider carefully how to protect the public from the vulnerabilities arising from the NII, but as with few other innovations, the NII and its inevitable counterparts will affect the entire global community. The real nub of the problem is that even a national legal system that directly addresses the NII issues will be only marginally beneficial if international norms of behavior do not develop.

The central problem is ambiguity. The threats of cyberspace are less coherent, less tangible, and certainly less foreseeable, than military confrontation. More to the point, international coalitions traditionally flow from military bases; a coalition based on cyberspace threats would represent a quantum leap in international investigatory cooperation. Traditional, but outmoded concepts of strength and vulnerability ranging from the military to gross national product, will inevitably obscure the contemporary reality of the power of information.

Unfortunately, international computer offenses are easier to commit than traditional international crimes, if for no other reason than that they require little in the way of manpower and resources. A destructive attack on the NII could be carried out as a means of warfare or terrorism with little risk of instigating physical conflict and possibly even without source detection. There are no visa or passport requirements and no checkpoints, only keystrokes. Moreover, few nations adequately guard against the harm. Even the United States, easily the most computer-organized nation in the world, is poorly mobilized for computer attacks.

NII disruption has the potential, if not the certainty, of springing forth quickly, dramatically, and destructively. The potential for economic abuse, sabotage, theft, and common crime is disturbing. Moreover, the problems created by a global NII attack would transcend all boundaries, confuse cultural mores, and confound contemporary laws. Because simple keystrokes can generate propaganda, enflame passions, or create artificial fears, the further potential for undermining the cohesiveness of national and international social structures is frightening.

The threat is particularly disquieting for developing nations

that still have loose bonds of social cohesion. Efforts of developed nations to protect social values from harm via the Internet speak eloquently to the proposition that cultural, social, economic, even military strengths potentially can be undermined by abusing digital technology. Of course, the other side of that coin is that modern communications, appropriately encouraged and protected, can contribute to the growth of democratic concepts.

IV. *A PAUCITY OF LAW*

Most nations have no laws against breaking into computers and those that do generally have only weak ones. The few with strong laws find implementation difficult because of the need for the still distant goal of international cooperation. Worse, some nations seem to tolerate the venality of computer hacking. The United States has, for example, identified overt bulletin boards in several nations, easily accessed, that are being used to develop and perfect viruses, propagate copyrighted programs, and frustrate intellectual property rights.

The first problem of international cooperation is simply to define the problem. The United States has a plethora of relevant laws which may or may not apply to a particular NII attack, and most nations are even more deficient. We are already at a point in history when cybertechnology requires an international understanding of the problem and a common frame of reference for combatting it. None now exists.

An oversimplistic statement of a second problem is venue. Traditionally, legal venue is found at the situs of an event, or in a res, or with a person. If an offense has an international dimension, venue may lie in the country where the offender is located, where the victim may be, or, occasionally, even in the nation through which the communications travel. Technology, however, has begun to confuse jurisdiction and venue because cyberspace crimes inevitably will transcend national and international boundaries.

More than the problem of international narcotics trafficking, more than weapons proliferation, more than international terrorism, the NII threat cannot be confronted effectively without close and concerted international cooperation and similar laws. Foreign nations generally must have similar law before

they will agree to cooperate, extradite, or expel the offender, and frequently they are very reluctant to relinquish their own nationals for foreign punishment.

To illustrate the fundamental need for cooperation, consider first a purely domestic attack on a defense computer system. Assuming the attack is detectable, it is still unlikely that a sophisticated intruder will leave an audit trail. The conduit of attack may lead across several state lines, requiring a trace of calls across state borders, and even, perhaps, through several carrier systems.

This frustrates beyond current legal procedure the traditional concepts of judicial warrant. Presumably the United States could, and should, ameliorate this problem with legislation to create some sort of national warrant process. That may be a daunting challenge, but not half so daunting as the international dimension. There exists now a facile ability to route an attack through multiple nations, making effective investigation improbable. On a positive note, the Council of Europe is addressing procedural problems of cyberinvestigation, such as how quickly to "trap and trace" an attack.

The problem, however, transcends both law and technology. Even assuming that legal norms come into being, common international social structures must exist to permit the law to work. A reasonably common international security architecture is needed. Ethical responsibility will be a common educational requirement, but one requiring individual national initiative. There is a need to put international flesh on skeletal concepts of privacy, confidentiality, and emergency response. Only with an underpinning of global involvement can there be an effective oversight and enforcement mechanism.

The United States laid these issues on the table at the 1995 G-7 Ministerial Conference on the Information Society. The G-7 agreed to find creative, technological and policy solutions to improve "the reliability and security of national and international networks . . . by developing security principles that are commensurate with the risk and magnitude of harm."[17]

The problem, however, requires more than an articulation of goals, it requires urgent action. Whereas most international

17. Exec. Office of the President, National Information Infrastructure: Draft Report on "NII Security: The Federal Role," 60 Fed. Reg. 32,038 (1995).

problems grow somewhat slowly, this one will not. The developments of cybertechnology and the NII are moving forward at warp speed while national and international efforts to meet the threat creep. Worse, because international cooperation is a *sine qua non* of remedy, the ability to confront the issue will grow at the speed of the slowest participant.

A parallel effort is needed both within and between nations. Governments must take the lead in serving as facilitators for promoting private sector responsibility. Critical research for security and assessment of public needs will require governmental resources. Governments themselves must be model users of the NII.

No doubt the potential dangers from sheer chaos that may result from disruption of computer systems will lead eventually to international norms of behavior. At present, however, a marginal tolerance for electronic burglary is a price that is being paid for the ability to assimilate vast quantities of data, to communicate instantaneously world-wide and to control governmental and public service activities.

When the tolerance level has been reached, nations will begin more seriously to look for a remedy. Finding national remedies necessary but individually deficient, they will turn toward an international remedy. In that venue, unlike most international problems, they will find law to be the one viable avenue of approach.

Diplomacy, economic coercion, and other traditional approaches will be singularly unhelpful. In the final analysis, the commonality of access and of international interdependence on the NII will require a commonality in goals, remedies, and responsive investigative techniques. Only a concerted effort to develop international legal norms holds the potential for any measure of investigatory or remedial success.

International law can make a difference. More to the point, only international norms of behavior can offer any realistic measure of protection against the global potential for harm. With the certainty of death and taxes, the day will come when international law turns to the task already at hand; the fundamental question is whether an electronic Pearl Harbor will be a global prerequisite.